An Introduction to Gröbner Bases

William W. Adams
Philippe Loustaunau

Graduate Studies in Mathematics
Volume 3

American Mathematical Society

http://dx.doi.org/10.1090/gsm/003

Selected Titles in This Series

13 **Paul C. Shields,** The ergodic theory of discrete sample paths, 1996
12 **N. V. Krylov,** Lectures on elliptic and parabolic equations in Hölder spaces, 1996
11 **Jacques Dixmier,** Enveloping algebras, 1996 Printing
10 **Barry Simon,** Representations of finite and compact groups, 1996
9 **Dino Lorenzini,** An invitation to arithmetic geometry, 1996
8 **Winfried Just and Martin Weese,** Discovering modern set theory. I: The basics, 1996
7 **Gerald J. Janusz,** Algebraic number fields, second edition, 1996
6 **Jens Carsten Jantzen,** Lectures on quantum groups, 1996
5 **Rick Miranda,** Algebraic curves and Riemann surfaces, 1995
4 **Russell A. Gordon,** The integrals of Lebesgue, Denjoy, Perron, and Henstock, 1994
3 **William W. Adams and Philippe Loustaunau,** An introduction to Gröbner bases, 1994
2 **Jack Graver, Brigitte Servatius, and Herman Servatius,** Combinatorial rigidity, 1993
1 **Ethan Akin,** The general topology of dynamical systems, 1993

An Introduction to Gröbner Bases

William W. Adams
Philippe Loustaunau

Graduate Studies
in Mathematics

Volume 3

American Mathematical Society

2000 *Mathematics Subject Classification.* Primary 13P10.

ABSTRACT. Gröbner bases are the primary tool for doing explicit computations in polynomial rings in many variables. In this book we give a leisurely introduction to the subject and its applications suitable for students with a little knowledge of abstract and linear algebra. The book contains not only the theory over fields, but also, the theory in modules and over rings.

Library of Congress Cataloging-in-Publication Data

Adams, William W., 1937–
An introduction to Gröbner bases/William W. Adams, Philippe Loustaunau.
p. cm. — (Graduate studies in mathematics, ISSN 1065-7339; 3)
Includes bibliographical references and index.
ISBN 0-8218-3804-0
1. Gröbner bases. I. Loustaunau, Philippe, 1958– . II. Title. III. Series.

QA251.3.A32 1994
512′.4—dc20

94-19081
CIP

♾ The paper used in this book is acid-free and falls within the guidelines
established to ensure permanence and durability.
This publication was typeset by the authors, with assistance
from the American Mathematical Society, using $\mathcal{A}\!\mathcal{M}\!\mathcal{S}$-TeX,
the American Mathematical Society's TeX macro system.
Visit the AMS home page at `http://www.ams.org/`

10 9 8 7 6 5 4 15 14 13 12 11 10 09

To my wife Elizabeth
and our daughters Ruth and Sarah
WWA

To my wife Yvonne
and our children Eileen, Gareth, and Manon
PL

Contents

Preface

We wrote this book with two goals in mind:

(i) To give a leisurely and fairly comprehensive introduction to the definition and construction of Gröbner bases;

(ii) To discuss applications of Gröbner bases by presenting computational methods to solve problems which involve rings of polynomials.

This book is designed to be a first course in the theory of Gröbner bases suitable for an advanced undergraduate or a beginning graduate student. This book is also suitable for students of computer science, applied mathematics, and engineering who have some acquaintance with modern algebra. The book does not assume an extensive knowledge of algebra. Indeed, one of the attributes of this subject is that it is very accessible. In fact, all that is required is the notion of the ring of polynomials in several variables (and rings in general in a few places, in particular in Chapter 4) together with the ideals in this ring and the concepts of a quotient ring and of a vector space introduced at the level of an undergraduate abstract and linear algebra course. Except for linear algebra, even these ideas are reviewed in the text. Some topics in the later sections of Chapters 2, 3, and 4 require more advanced material. This is always clearly stated at the beginning of the section and references are given. Moreover, most of this material is reviewed and basic theorems are stated without proofs.

The book can be read without ever "computing" anything. The theory stands by itself and has important theoretical applications in its own right. However, the reader will not fully appreciate the power of, or get insight into, the methods introduced in the book without actually doing some of the computations in the examples and the exercises by hand or, more often, using a Computer Algebra System (there are over 120 worked-out examples and over 200 exercises). Computing is useful in producing and analyzing examples which illustrate a concept already understood, or which one hopes will give insight into a less well understood idea or technique. *But the real point here is that computing is the very essence of the subject.* This is why Gröbner basis theory has become a major research area in computational algebra and computer science. Indeed, Gröbner basis theory is generating increasing interest because of its usefulness in providing computational tools which are applicable to a wide range of problems in mathematics, science, engineering, and computer science.

Gröbner bases were introduced in 1965 by Bruno Buchberger[1] [**Bu65**]. The basic idea behind the theory can be described as a generalization of the theory of polynomials in one variable. In the polynomial ring $k[x]$, where k is a field, any ideal I can be generated by a single element, namely the greatest common divisor of the elements of I. Given any set of generators $\{f_1, \ldots, f_s\} \subseteq k[x]$ for I, one can compute (using the Euclidean Algorithm) a single polynomial $d = \gcd(f_1, \ldots, f_s)$ such that $I = \langle f_1, \ldots, f_s \rangle = \langle d \rangle$. Then a polynomial $f \in k[x]$ is in I if and only if the remainder of the division of f by d is zero. Gröbner bases are the analog of greatest common divisors in the multivariate case in the following sense. A Gröbner basis for an ideal $I \subseteq k[x_1, \ldots, x_n]$ generates I and a polynomial $f \in k[x_1, \ldots, x_n]$ is in I if and only if the remainder of the division of f by the polynomials in the Gröbner basis is zero (the appropriate concept of division is a central aspect of the theory).

This abstract characterization of Gröbner bases is only one side of the theory. In fact it falls far short of the true significance of Gröbner bases and of the real contribution of Bruno Buchberger. Indeed, the ideas behind the abstract characterization of Gröbner bases had been around before Buchberger's work. For example, Macaulay [**Mac**] used some of these ideas at the beginning of the century to determine certain invariants of ideals in polynomial rings and Hironaka [**Hi**], in 1964, used similar ideas to study power series rings. But the true significance of Gröbner bases is the fact that they can be computed. Bruno Buchberger's great contribution, and what gave Gröbner basis theory the status as a subject in its own right, is his algorithm for computing these bases.

Our choice of topics is designed to give a broad introduction to the elementary aspects and applications of the subject. As is the case for most topics in commutative algebra, Gröbner basis theory can be presented from a geometric point of view. We have kept our presentation algebraic except in Sections 1.1 and 2.5. For those interested in a geometric treatment of some of the theory we recommend the excellent book by D. Cox, J. Little and D. O'Shea [**CLOS**]. The reader who is interested in going beyond the contents of this book should use our list of references as a way to access other sources. We mention in particular the books by T. Becker and V. Weispfenning [**BeWe**] and by B. Mishra [**Mi**] which contain a lot of material not in this book and have extensive lists of references on the subject.

Although this book is about computations in algebra, some of the issues which might be of interest to computer scientists are outside the scope of this book. For example, implementation of algorithms and their complexity are discussed only briefly in the book, primarily in Section 3.3. The interested reader should consult the references.

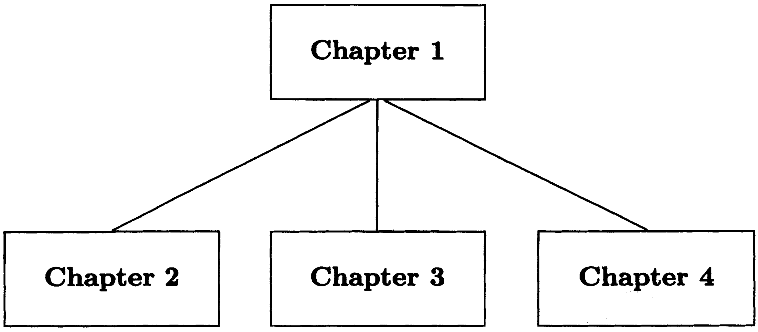
[1] Wolfgang Gröbner was Bruno Buchberger's thesis advisor.

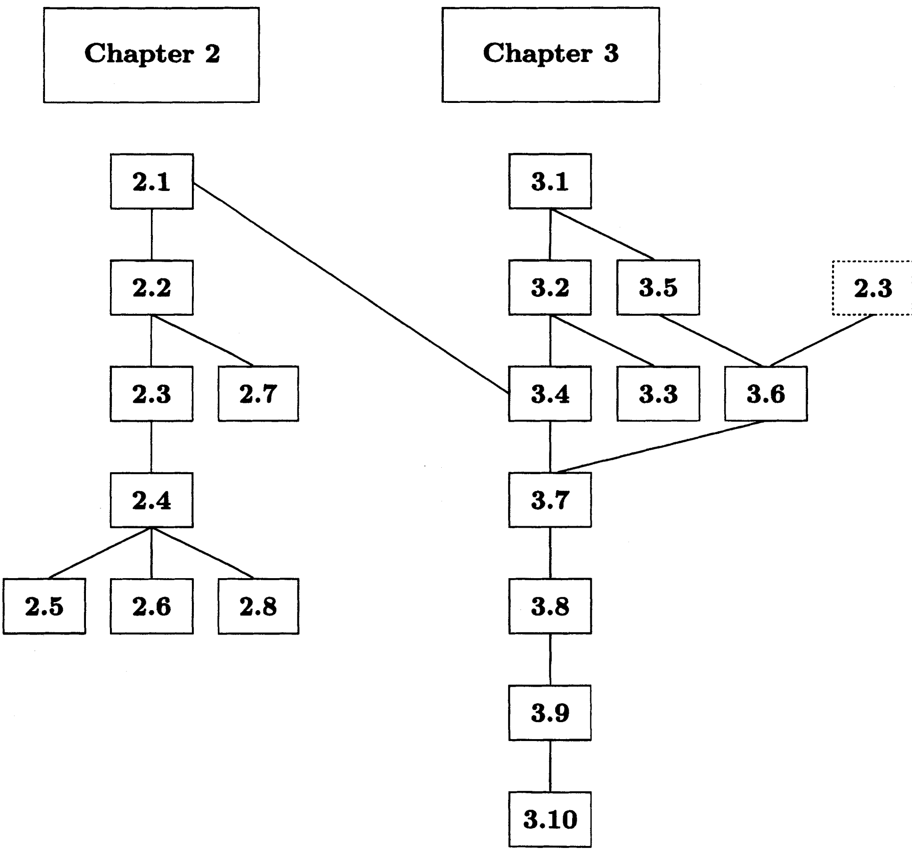
In Chapter 1 we give the basic introduction to the concept of a Gröbner basis and show how to compute it using Buchberger's Algorithm. We are careful to give motivations for the definition and algorithm by giving the familiar examples of Gaussian elimination for linear polynomials and the Euclidean Algorithm for polynomials in one variable. In Chapter 2 we present the basic applications to algebra and elementary algebraic geometry. We close the chapter with three specialized applications to algebra, graph theory, and integer programming. In Chapter 3 we begin by using the concept of syzygy modules to give an improvement of Buchberger's Algorithm. We go on to show how to use Gröbner bases to compute the syzygy module of a set of polynomials (this is solving diophantine equations over polynomial rings). We then develop the theory of Gröbner bases for finitely generated modules over polynomial rings. With these, we extend the applications from the previous chapter, give more efficient methods for computing some of the objects from the previous chapter, and conclude by showing how to compute the Hom functor and free resolutions. In Chapter 4 we develop the theory of Gröbner bases for polynomial rings when the coefficients are now allowed to be in a general Noetherian ring and we show how to compute these bases (given certain computability conditions on the coefficient ring). We show how the theory simplifies when the coefficient ring is a principal ideal domain. We also give applications to determining whether an ideal is prime and to computing the primary decomposition of ideals in polynomial rings in one variable over principal ideal domains.

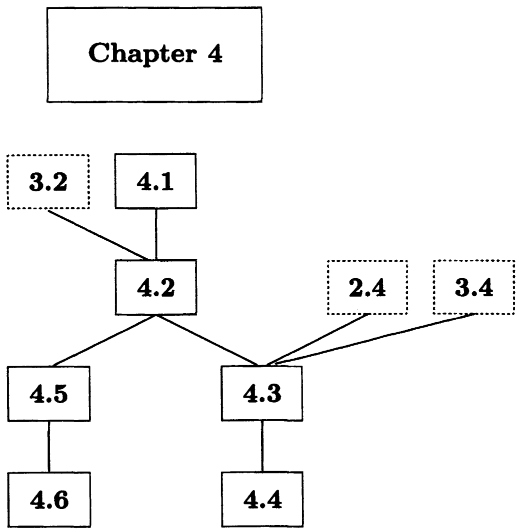
We give an outline of the section dependencies at the end of the Preface. After Chapter 1 the reader has many options in continuing with the rest of the book. There are exercises at the end of each section. Many of these exercises are computational in nature, some doable by hand while others require the use of a Computer Algebra System. Other exercises extend the theory presented in the book. A few harder exercises are marked with (*).

This book grew out of a series of lectures presented by the first author at the National Security Agency during the summer of 1991 and by the second author at the University of Calabria, Italy, during the summer of 1993.

We would like to thank many of our colleagues and students for their helpful comments and suggestions. In particular we would like to thank Beth Arnold, Ann Boyle, Garry Helzer, Karen Horn, Perpetua Kessy, Lyn Miller, Alyson Reeves, Elizabeth Rutman, Brian Williams, and Eric York. We also want to thank Sam Rankin, Julie Hawks and the AMS staff for their help in the preparation of the manuscript.


Chapter 1
Chapter 2
Chapter 3
Chapter 4


Chapter 2
Chapter 3
2.1
2.2
2.3
2.7
2.4
2.5
2.6
2.8
3.1
3.2
3.5
2.3
3.4
3.3
3.6
3.7
3.8
3.9
3.10


Chapter 4
3.2
4.1
4.2
2.4
3.4
4.5
4.3
4.6
4.4

References

[AdGo] W.W. Adams and L.J. Goldstein, *Introduction to Number Theory,* Prentice Hall, Englewood Cliffs, NJ, 1976.

[AtMD] M.F. Atiyah and I.G. MacDonald, *Introduction to Commutative Algebra,* Addison-Wesley, Reading, MA, 1969.

[Ba] D. Bayer, *The Division Algorithm and the Hilbert Scheme,* Ph.D. Thesis, Harvard University, Cambridge, MA, 1982.

[BaSt88] D.A. Bayer and M. Stillman, *On the complexity of computing syzygies,* J. Symb. Comp. **6** (1988), 135–147.

[BaSt90] D.A. Bayer and M. Stillman, *Macaulay: A system for computation in algebraic geometry and commutative algebra.* User's manual.

[BeWe] T. Becker and V. Weispfenning, *Gröbner Bases: A Computational Approach to Commutative Algebra,* Springer Verlag, Berlin and New York, 1993.

[Bu65] B. Buchberger, *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal,* Ph.D. Thesis, Inst. University of Innsbruck, Innsbruck, Austria, 1965.

[Bu79] B. Buchberger, *A criterion for detecting unnecessary reductions in the construction of Gröbner bases,* in EUROSAM'79, An International Symposium on Symbolic and Algebraic Manipulation (E.W. Ng, ed.), Lecture Notes in Comput. Sci., vol. 72, Springer Verlag, Berlin and New York, 1979, 3–21.

[Bu83] B. Buchberger, *A note on the complexity of constructing Gröbner bases,* in EUROCAL'83, European Computer Algebra Conference (J.A. van Hulzen ed.), Lecture Notes in Comput. Sci., vol. 162, Springer Verlag, Berlin and New York, 1983, 137–145.

[Bu85] B. Buchberger, *Gröbner bases: An algorithmic method in polynomial ideal theory,* in Multidimensional Systems Theory (N.K. Bose ed.), Reidel, Dordrecht, 1985, 184–232.

[CGGLMW] B. Char, K. Geddes, G. Gonnet, B. Leong, M. Monogan, and S.M. Watt, *Maple V Library Reference Manual,* Springer Verlag, Berlin and New York, 1991.

[Coh] H. Cohen, *A Course in Computational Algebraic Number Theory,* Springer Verlag, Berlin and New York, 1993.

[CoTr] P. Conti and C. Traverso, *Buchberger algorithm and integer programming,* in Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes AAECC'9 (H.F. Mattson, T. Mora, and T.R.N Rao eds.), Lecture Notes in Comput. Sci., vol. 539, Springer verlag, Berlin and New York, 1991, 130–139.

[CLOS] D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra,* Springer Verlag, Berlin and New York, 1992.

[Cz] S.R. Czapor, *Gröbner basis methods for solving algebraic equations,* Ph.D. Thesis, University of Waterloo, Canada, 1988.

[EHV] D. Eisenbud, C. Huneke, and W. Vasconcelos, *Direct methods for primary decomposition,* Invent. Math. **110** (1992), 207-235.

[FGLM] J.C. Faugère, P. Gianni, D. Lazard, and T. Mora, *Efficient computation of zero-dimensional Gröbner bases by change of ordering,* J. Symb. Comp. **16** (1993), 329–344.

[Ga] D. Gale, *The Theory of Linear Economic Models,* McGraw-Hill, New York, 1960.

[GTZ] P. Gianni, B. Trager, and G. Zacharias, *Gröbner bases and primary decomposition of polynomial ideals,* J. Symb. Comp. **6** (1988), 149–167.

[GMNRT] A. Giovini, T. Mora, G. Niesi, L. Robbiano, and C. Traverso, *"One sugar cube, please" or selection strategies in the Buchberger algorithm,* in Proc. International Symposium on Symbolic and Algebraic Computation ISSAC'91 (S.M. Watt ed.), ACM Press, New York, 1991, 49–54.

[GiNi] A. Giovini and G. Niesi, *CoCoA user manual,* 1990.

[Go] L. J. Goldstein, *Abstract Algebra, a First Course,* Prentice Hall, Englewood Cliffs, NJ, 1973.

[He] I.N. Herstein, *Topics in Algebra,* Blaisdell, New York, 1964.

[Hi] H. Hironaka, *Resolution of singularities of an algebraic variety over a field of characteristic zero,* Ann. Math. **79** (1964), 109–326.

[Hun] T.W. Hungerford, *Algebra,* Springer Verlag, Berlin and New York, 1974.

[Huy] D.T. Huynh, *A superexponential lower bound for Gröbner bases and Church-Rosser commutative Thue systems,* Inf. Contr. **68** (1986), 196–206.

[JeSu] R.D. Jenks and R.S. Sutor, *AXIOM: The Scientific Computation System,* Springer Verlag, Berlin and New York, 1992.

[Lak] Y.N. Lakshman, *On the complexity of computing Gröbner bases for zero-dimensional polynomials ideals,* Ph.D. Thesis, Rensselaer Polytechnic Institute, Troy, NY, 1990.

[Lan] S. Lang, *Algebra,* Addison-Wesley, Reading, MA, 1970.

[Laz85] D. Lazard, *Ideal bases and primary decomposition: Case of two variables,* J. Symb. Comp. **1** (1985), 261–270.

[Laz91] D. Lazard, *Systems of algebraic equations (algorithms and complexity),* Computational Algebraic Geometry and Commutative Algebra (D. Eisenbud and L. Robbiano, eds.), Cambridge University Press, London, 1993.

[Mac] F.S. Macaulay, *Some properties of enumeration in the theory of modular systems,* Proc. London Math. Soc. **26** (1927), 531–555.

[MaMe] E.W. Mayr and A.R Meyer, *The complexity of the word problems for commutative semigroups and polynomial ideals,* Adv. Math **46** (1982), 305–329.

[Mi] B. Mishra, *Algorithmic Algebra,* Springer Verlag, Berlin and New York, 1993.

[Mö88] H.M. Möller, *On the construction of Gröbner bases using syzygies,* J. Symb. Comp. **6** (1988), 345–359.

[Mö90] H.M. Möller, *Computing syzygies a la Gauss Jordan,* in Effective Methods in Algebraic Geometry (T. Mora and C. Traverso, eds.), Progress in Mathematics **94**, Birkhäuser Verlag, Basel, 1990, 335–345.

[MöMo] H.M. Möller and T. Mora, *New constructive methods in classical ideal theory,* J. Algebra **100** (1986), 138–178.

[MoRo] T. Mora and L. Robbiano, *The Gröbner fan of an ideal,* J. Symb. Comp. **6** (1988), 183–208.

[NZM] I. Niven, H.S. Zuckerman, and H.L. Montgomery, *An Introduction to the Theory of Numbers,* 5th ed., Wiley, New York, 1991.

[RoSw] L. Robbiano and M. Sweedler, *Subalgebra bases,* in Proc. Commutative Algebra Salvador (W. Burns and A. Simis eds.), Lecture Notes in Math., vol. 1430, Springer Verlag, Berlin and New York, 1988, 61–87.

[Schre] F.O. Schreyer, *Die Berechnung von Syzygien mit dem verallgemeinerten Weierstrasschen Divisionsatz,* Diplomarbeit, Hamburg, 1980.

[Schri] A. Schrijver, *Theory of Linear and Integer Programming,* Wiley, Chichester, NY, 1986.

[Se] A. Seidenberg, *Constructions in algebra,* Trans. Amer. Math. Soc. **197** (1974), 272–313.

[ShSw] D. Shannon and M. Sweedler, *Using Gröbner bases to determine algebra membership, split surjective algebra homomorphisms determine birational equivalence,* J. Symb. Comp. **6** (1988), 267–273.

[Sz] G. Szekeres, *A canonical basis for the ideals of a polynomial domain,* Am. Math. Mon. **59** (1952), 379–386.

[Wo] S. Wolfram, *Mathematica: A System for Doing Mathematics by Computer,* Addison-Wesley, Reading, MA, 1991.

[Za] G. Zacharias, *Generalized Gröbner bases in commutative polynomial rings,* Bachelor's Thesis, MIT, Cambridge, MA, 1978.

List of Symbols

$\mathbb{N}$	natural numbers
$\mathbb{Z}$	ring of integers
$\mathbb{Z}_n$	ring of integers modulo n
$\mathbb{Q}$	field of rational numbers
$\mathbb{R}$	field of real numbers
$\mathbb{C}$	field of complex numbers
$\mathbb{T}^n$	set of power products in the variables $x_1, \ldots, x_n$
k	a field
k^n	affine space
$k[x_1, \ldots, x_n]$	ring of polynomials in the variables $x_1, \ldots, x_n$ with coefficients in the field k
$\langle f_1, \ldots, f_s \rangle$	ideal (submodule) generated by $f_1, \ldots, f_s$
$f \equiv g \pmod{I}$	f congruent to g modulo I
$k[x_1, \ldots, x_n]/I$	quotient ring of $k[x_1, \ldots, x_n]$ by the ideal I
$f + I$	coset of f modulo I
$V(S)$	variety in k^n defined by the set of polynomials S
$V(f_1, \ldots, f_s)$	variety in k^n defined by the polynomials $f_1, \ldots, f_s$
$I(V)$	ideal in $k[x_1, \ldots, x_n]$ defined by $V \subseteq k^n$
$\langle S \rangle$	ideal generated by the polynomials in the set S
gcd	greatest common divisor
lcm	least common multiple
$\dim_k(L)$	dimension of the k-vector space L
$\mathrm{lt}(f)$	leading term of f
$\mathrm{lp}(f)$	leading power product of f
$\mathrm{lc}(f)$	leading coefficient of f
$\boldsymbol{x}^{\boldsymbol{\alpha}}$	$x_1^{\alpha_1} \cdots x_n^{\alpha_n}$
$f \xrightarrow{G} h$	f reduces to h modulo G in one step
$f \xrightarrow{G}_+ h$	f reduces to h modulo G

$f \xrightarrow{X,g} h$	f reduces to h and $h = f - Xg$
$\mathrm{Lt}(S)$	leading term ideal (submodule) defined by S
$S(f,g)$	S-polynomial of f and g
$N_G(f)$	normal form of f with respect to G
$V_K(S)$	variety in K^n defined by $S \subseteq k[x_1, \dots, x_n]$
$\overline{k}$	algebraic closure of the field k
$\sqrt{I}$	radical of the ideal I
$I \cap J$	intersection of I and J
$I \colon J$	ideal quotient of I by J
$\mathrm{im}(\phi)$	image of the map ϕ
$\ker(\phi)$	kernel of the map ϕ
$k[f_1, \dots, f_s]$	k-algebra generated by the polynomials $f_1, \dots, f_s$
$k[F]$	k-algebra generated by the polynomials in the set F
$k(x_1, \dots, x_n)$	rational function field
$k(\alpha)$	field extension of k obtained by adjoining α
$k(\alpha_1, \dots, \alpha_n)$	field extension of k obtained by adjoining $\alpha_1, \dots, \alpha_n$
A^m	set of column vectors with entries in the ring A
M/N	quotient module of M by N
$\cong$	isomorphic to
$\boldsymbol{e}_1, \dots, \boldsymbol{e}_m$	standard basis for the free module A^m
$\begin{bmatrix} f_1 & \cdots & f_s \end{bmatrix}$	$1 \times s$ matrix whose entries are polynomials $f_1, \dots, f_s$
$\begin{bmatrix} \boldsymbol{f}_1 & \cdots & \boldsymbol{f}_s \end{bmatrix}$	$m \times s$ matrix whose columns are vectors $\boldsymbol{f}_1, \dots, \boldsymbol{f}_s$
$\mathrm{Syz}(f_1, \dots, f_s)$	syzygy module of the matrix $\begin{bmatrix} f_1 & \cdots & f_s \end{bmatrix}$
$\mathrm{Syz}(F)$	syzygy module of the matrix F
$\mathrm{lm}(\boldsymbol{f})$	leading monomial of the vector $\boldsymbol{f}$
$F \oplus G$	direct sum of the matrices F and G
$[F\|G]$	concatenation of the matrices F and G
${}^tS$	transpose of the matrix S
$\mathrm{ann}(M)$	annihilator of the module M
$F \otimes G$	tensor product of the matrices F and G
$\mathrm{Hom}(M,N)$	set of all A-module homomorphisms between M and N
$\langle U \rangle$	module generated by the columns of the matrix U
$S^{-1}A$	localization of the ring A at the multiplicative set S
A_P	localization of the ring A at the prime ideal P
A_g	localization of the ring A at the set $\{1, g, g^2, g^3, \dots\}$

Index

A very carefully crafted introduction to the theory and some of the applications of Gröbner bases ... contains a wealth of illustrative examples and a wide variety of useful exercises, the discussion is everywhere well-motivated, and further developments and important issues are well sign-posted ... has many solid virtues and is an ideal text for beginners in the subject ... certainly an excellent text.

—Bulletin of the London Mathematical Society

As the primary tool for doing explicit computations in polynomial rings in many variables, Gröbner bases are an important component of all computer algebra systems. They are also important in computational commutative algebra and algebraic geometry. This book provides a leisurely and fairly comprehensive introduction to Gröbner bases and their applications. Adams and Loustaunau cover the following topics: the theory and construction of Gröbner bases for polynomials with coefficients in a field, applications of Gröbner bases to computational problems involving rings of polynomials in many variables, a method for computing syzygy modules and Gröbner bases in modules, and the theory of Gröbner bases for polynomials with coefficients in rings. With over 120 worked-out examples and 200 exercises, this book is aimed at advanced undergraduate and graduate students. It would be suitable as a supplement to a course in commutative algebra or as a textbook for a course in computer algebra or computational commutative algebra. This book would also be appropriate for students of computer science and engineering who have some acquaintance with modern algebra.

ISBN 978-0-8218-3804-4

9 780821 838044

GSM/3